FACULTY OF
BUSINESS AND
ECONOMICS

MACQUARIE
University

Group assessment cover sheet

Unit code	8014	**Due date**	19.10.25
Group name or number *if applicable*	23		
Turnitin # *if applicable*		**Assessment #** *if applicable*	
Assessment topic	Assessment 2 - Group Project		

Group members (please write clearly in capital letters)

Number	Student ID	Class time	Class room	Tutor
1	48312932	6:00 PM - 9:00 PM	nce Decisions Lab, (	Dr Nihad Aliyev
2	48614086	6:00 PM - 9:00 PM	nce Decisions Lab, (	Dr Nihad Aliyev
3	48657816	6:00 PM - 9:00 PM	nce Decisions Lab, (	Dr Nihad Aliyev
4	48457515	6:00 PM - 9:00 PM	nce Decisions Lab, (	Dr Nihad Aliyev
5	48444030	6:00 PM - 9:00 PM	nce Decisions Lab, (	Dr Nihad Aliyev
6				

All group members must sign the declaration overleaf.

* Assessments will be sorted for return according to the group name or number (if allocated) or the student number of the group member listed at 1 above.

This coversheet is for use with all assessments submitted in BESS (E4B106):

businessandeconomics.mq.edu.au/for/new_and_current_students/undergraduate/bess

Declaration

We certify that:

- This assessment is our group's work, based on our personal study and/or research;
- We have acknowledged all material and sources used in the preparation of this assessment, including any material generated in the course of our employment;
- Neither the assessment, nor substantial parts of it, have been previously submitted for grading in this or any other institution;
- We have not copied in part, or in whole, or otherwise plagiarized the work of other students;
- We have read and we understand the criteria used for assessment;
- The assessment is within the word and page limits specified in the unit outline;
- The use of any material in this assessment does not infringe the intellectual property /copyright of a third party;
- We understand that this assessment may undergo electronic detection for plagiarism, and a copy of the assessment may be retained in a database and used to make comparisons with other assessments in future. *Work retained in a database is anonymous and will not be able to be matched to individual students*;
- We take full responsibility for the correct submission of this assessment in the appropriate place with the correct cover sheet attached and we have retained a duplicate copy of this assessment.

Number	Student name	Signature	Date
1	Muntasir Md Nafis		18 / 10 25
2	Pranjal Joshi	Pranjal	18 / 10 / 25
3	Raisa Rahman	Raisa.	18 / 10 / 25
4	Ridwan Bin Khalid		18 / 10 / 25
5	Afi Noor	Afi	18 / 10 / 25
6			18 / 10 / 25

This declaration is a summary of the University policy on plagiarism. For the policy in full, please refer to Student Information in the Handbook of Undergraduate Studies or **mq.edu.au/policy/docs/academic_honesty/policy.html**

MARKER'S COMMENTS

GRADE

Table of Contents

Executive Summary

This report analyses Fireblocks, a leading financial technology company that provides secure infrastructure for institutions to hold, move, and manage digital assets. Founded in 2018 by cybersecurity experts, Fireblocks enables banks, fintechs, and payment providers to transact safely using advanced technologies such as multi-party computation (MPC) and confidential computing. These innovations eliminate single points of failure, enhance compliance, and build institutional trust in digital finance.

The report examines Fireblocks' products, emerging technologies, target markets, regulatory alignment, and key business risks. Its growing network of over 2,000 institutional clients, integration with global regulatory frameworks (AUSTRAC, MAS, FCA, and MiCA), and partnerships with major financial institutions highlight its scalability and resilience.

Fireblocks' competitive advantage lies in its strong security architecture, RegTech integration, and cooperative partnerships with traditional financial institutions. The analysis concludes that Fireblocks demonstrates exceptional long term growth potential and represents a high value investment opportunity for investors seeking exposure to the secure and expanding digital asset economy.

Introduction

The cryptocurrency landscape has undergone a significant transformation in recent years, evolving from a niche interest into a mainstream financial sector and as of October 2025, the global cryptocurrency market capitalization has experienced significant growth, reaching approximately $3.8 trillion (Economic Times,2025). This report examines one of the many key contributors of this explosive growth: Fireblocks, a financial technology company that provides secure infrastructure for holding, moving, and using digital assets for institutions. Fireblocks' platform includes custody, wallet-as-a-service, payments, tokenization, and a network that connects counterparties so they can transact with strong controls and faster settlement times. These capabilities make Fireblocks a useful case study for how digital asset infrastructure is being adopted by banks, payment providers, fintechs, and Web3 firms.

We situate Fireblocks within the broader fintech landscape, where technology is reshaping how money is stored, moved, and managed. By focusing on Fireblocks, the report explores how one firm's infrastructure stack addresses security and operational needs that arise when institutions handle digital assets. Our aim is to provide a clear, neutral foundation for analysis of technology, market fit, regulation, competition, and risks so that potential investors can gather value from it and make the right investment calls based on their requirements.

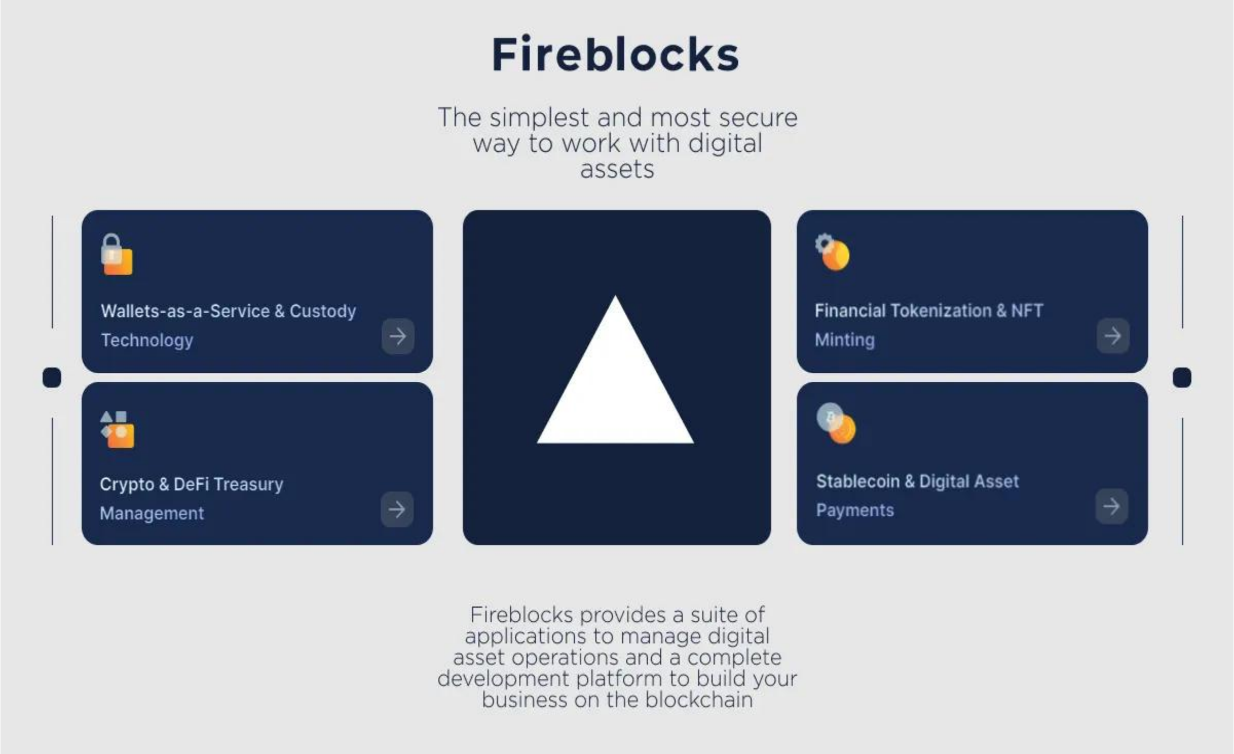
Company Overview

Founded in 2018 by three cybersecurity experts, Fireblocks is a US-based company that helps businesses safely hold, move, and use digital assets such as cryptocurrencies and stablecoins. In simple terms, it provides wallets and rails that banks, fintechs, payment companies, and crypto firms need to operate with strong controls. The company states its mission as "Enable every business to easily and securely support digital assets and cryptocurrencies" (Fireblocks, 2025a).

Fireblocks offers secure custody, wallet-as-a-service, payments, tokenization, and a built-in network so customers can transact with each other quickly and reliably (Fireblocks, 2025b). At its core is a security approach called multi-party computation, which splits sensitive keys into pieces and removes a single point of failure (Fireblocks,2025c). It acts like a vault that needs several different keys and approvals before anything can move. In simpler terms, Fireblocks claim to provide a way for people to grow their business on the blockchain, protect their crypto assets, expand payment reach using stablecoins all while maintaining regulatory standards. They claim that more than 2,000 institutions use its network to transact daily, which shows how widely it is used in finance.

One of the big features of the platform is its ability to pay sellers in minutes using set rules such as “two managers must approve any transfer over 50,000 USD,” and send the payout over the Fireblocks Network to a seller’s exchange account. This can reduce costs and speed up settlement compared with traditional cross-border wires, while keeping a clear audit trail and strong approvals in place (Evans, 2025). In essence, Fireblocks gives mainstream companies a safer, simpler way to bring digital assets into everyday business operations.

Fireblocks gained global attention after raising 550 million USD in a 2022 Series E round that valued the company at about 8 billion USD (Forbes, 2022) and since its inception in 2018, Fireblocks’ platform has transferred over $2 trillion in digital assets and amassed $45 billion in custody.



Fireblocks

The simplest and most secure way to work with digital assets

Wallets-as-a-Service & Custody Technology

Crypto & DeFi Treasury Management

Financial Tokenization & NFT Minting

Stablecoin & Digital Asset Payments

Fireblocks provides a suite of applications to manage digital asset operations and a complete development platform to build your business on the blockchain

Figure 1: Overview of Fireblock’s product suite. (Kroweski, 2023)

Emerging Technologies of Fireblocks

Fireblocks' main competitive edge is its security at scale. It signs, stores, and moves digital assets while minimizing the risk of exposing private keys, and it forces policy checks before any transaction. Broadly it stands on four pillars - secure multi-party computation for threshold signatures, confidential key shares and signing code run in isolated hardware environments, broad blockchain connectivity that supports many chains and smart contracts, and finally an API-first integration layer and policy engine that lets institutions automate transfers, approvals, and DeFi actions under strict controls.

MPC-CMP Implementation

The main concept of Multi-Party Computation (MPC) algorithm is to split a private key into independent shares and sign without ever reconstructing the full key (Zhong et al., 2020). Fireblocks applies multi-party computation in a unique way through its **own invention** Multi-Party Computation - Cryptographic Message Protocol **(MPC-CMP)** protocol. This approach optimizes distributed key generation and signing by cutting the number of communication rounds between cosigners, allowing near-instant transaction approval without reassembling the private key. This optimization Fireblocks reported eight times faster signing, enabling scalability without reducing security (Marciano, 2025). Figure 2 shows this process during the onboarding of a new customer cosigner (either a new mobile device or a cosigner server) where new key shards are generated and distributed securely among cosigners (AWS, 2023).

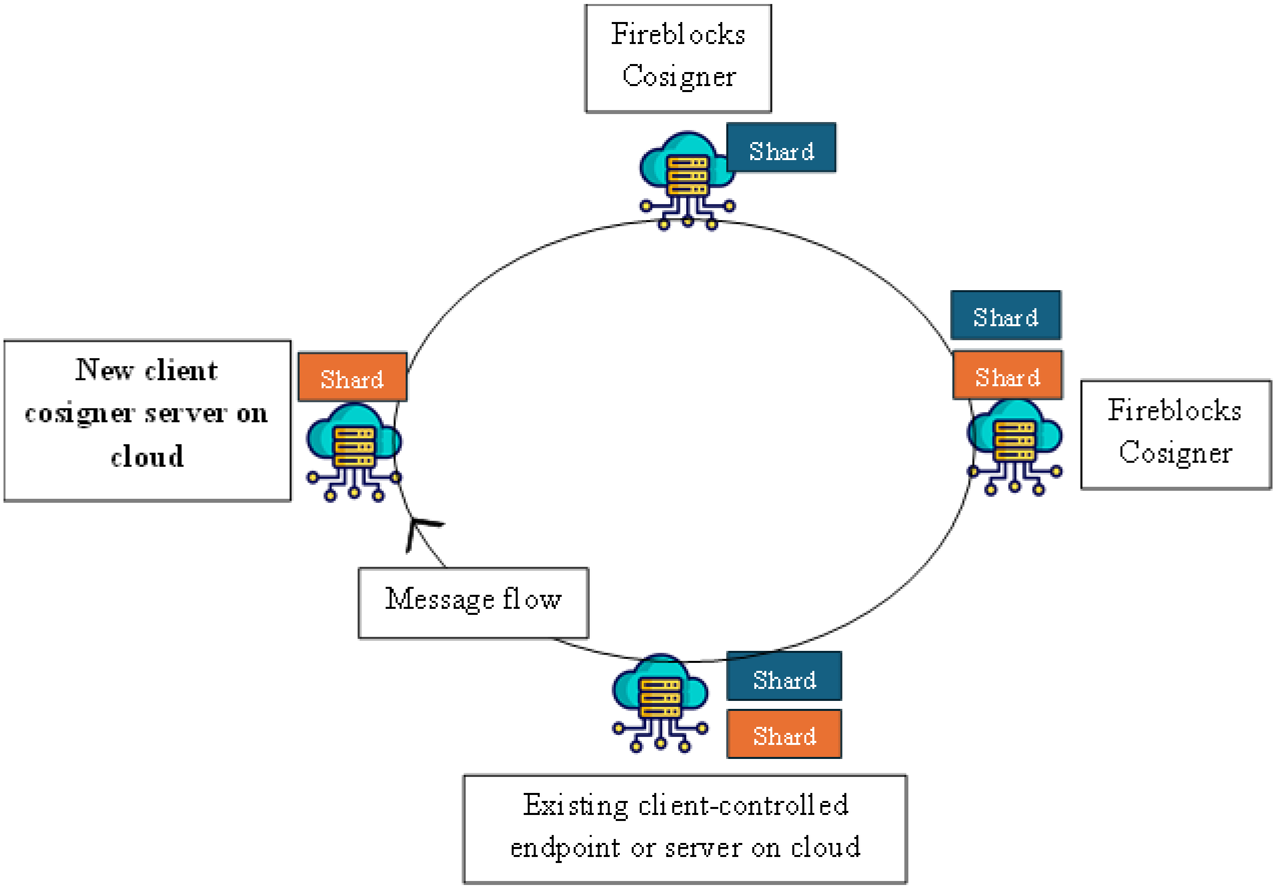
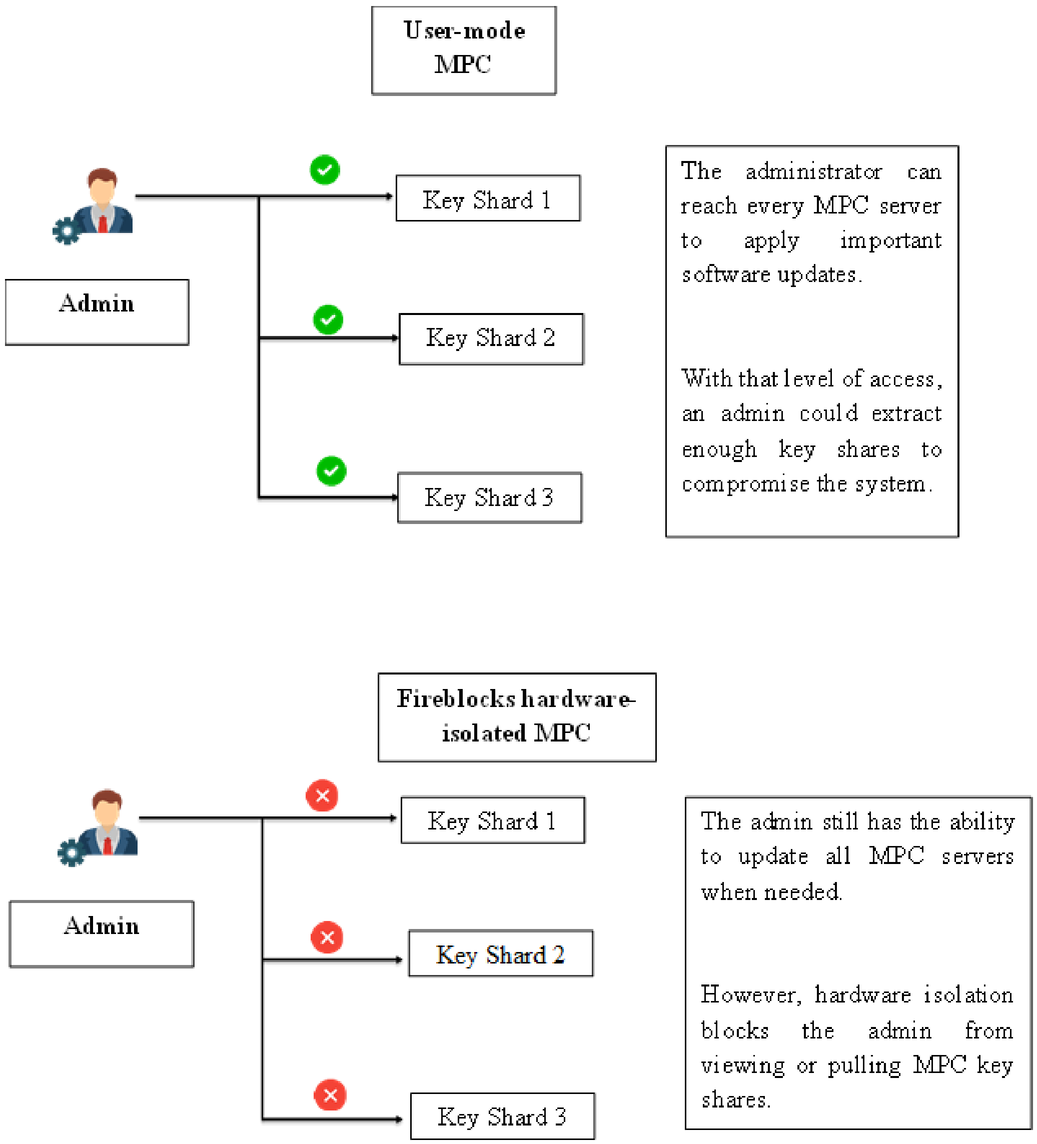

Fireblocks Cosigner
Shard
New client cosigner server on cloud
Shard
Shard
Shard
Fireblocks Cosigner
Message flow
Shard
Shard
Existing client-controlled endpoint or server on cloud

Figure 2: Onboarding process for a new customer cosigner during **secured** MPC-CMP key setup.

Hardware-isolated MPC

Fireblocks combines MPC with hardware security to further isolate sensitive operations. Customer cosigners can run inside AWS Nitro Enclaves or Azure SGX environments, so key shares and signing processes occur inside protected memory that even the cloud provider cannot access (AWS, 2023; Microsoft, 2024). As a result, they cannot be extracted even if malware or a hacker gains control over the server's operating system since the enclave's memory space and data remain encrypted as illustrated in figure 3.



The administrator can reach every MPC server to apply important software updates.

With that level of access, an admin could extract enough key shares to compromise the system.

The admin still has the ability to update all MPC servers when needed.

However, hardware isolation blocks the admin from viewing or pulling MPC key shares.

Figure 3: Comparison between user-mode MPC and Fireblocks' hardware-isolated MPC

Blockchain Connectivity, DeFi Integration, and API-First Automation

Fireblocks' blockchain connectivity and policy automation work together to create a unified operational framework. Through its chain-agnostic APIs, institutions can interact with multiple blockchains and decentralized finance protocols in a single, secure environment (Fireblocks, 2024). Tools such as Fireblocks Swaps and the Token Allowance Manager simplify on-chain actions and reduce smart contract risk, while the API-first policy engine automates transaction approvals, compliance checks, and governance workflows. Together, these capabilities not only streamline institutional engagement with blockchain ecosystems but also expand access to fintech for a wider range of users and organizations, lowering barriers to entry into the digital asset economy.

Technological Barriers and Challenges

Data Security and Privacy Risks: In traditional crypto wallets, the problem of key loss causing permanent asset loss has been frequent, but MPC reduces this single point of failure, allowing secure recovery through threshold approval (Lim et al., 2025). Fireblocks further strengthens this through MPC-CMP and hardware-isolated enclaves, ensuring that key shards remain encrypted even under system compromise. However, because of more secure infrastructure offering, large companies like Fireblocks attract a higher volume of customer funds. As a result, Fireblock is a more lucrative target for concentrated attacks (Erinle et al., 2025).

Scalability: As the number of cosigners, wallets, and shards increases, the overhead for coordination, share generation, recovery and rotation becomes more complex. While the one-round signing is progress, other phases (key generation, rotation, user onboarding) still require communication and orchestration across nodes. On top of that, institutions increasingly want to operate across many blockchains. Each chain may have different signature schemes, transaction models, fee models and finality characteristics. Ensuring the infrastructure supports all of these without performance degradation under heavy load is a challenge.

Standardisation of protocols and interoperability: Without broad industry standards for distributed key-signing and threshold schemes, bespoke systems may be less interoperable. This slows adoption and scaling across institutional platforms.

Fireblocks’ Target Market

Fireblocks’ target market is institutional participants in the rapidly expanding crypto asset management and custody market, which forms a part of the larger digital asset economy. Its primary customers are financial institutions that hold, trade or process digital assets. These include global and regional banks, hedge funds, crypto exchanges, lending desks, asset managers and large fintech payment providers. By 2023, Fireblocks had more than 1,800 clients including major names such as Wordplay, Revolut, BNY Mellon, NAB and ANZ (Report: Fireblocks Business Breakdown & Founding Story | Contrary Research, 2018). These are organisations that demand enterprise-grade security, regulatory compliance and seamless integration into the blockchain networks.

Customer Segment	Core needs	Fireblocks' value offering
Banks and large financial firms	Need regulated and secure custody solutions with compliance and audit trails that integrate with legacy systems	Fireblocks offers digital wallets, policy and governance controls, transaction tracking, APIs to integrate with core banking systems
Crypto exchanges and trading desks	Move crypto quickly and securely between wallets, clients and partners; manage treasury and liquidity	Enables safe transfers, automated workflows, multi-chain support, and connectivity to liquidity partners
Hedge funds and investment managers	Want secure custody, reporting, governance over large crypto portfolios	Gives robust custody, permission controls, tools for treasury management
Fintechs and wallet providers	Want to offer crypto or token services for their customers	Offers Wallet as a Service, APIs, stablecoin payment

	without building full infrastructure themselves	rails, integration with Fireblocks Network
Lending desks and DeFi (decentralised finance) platforms	Need to move collateral and manage assets across different blockchains safely.	Helps them automate transfers, set internal rules, and manage risks.

Table 1: Fireblocks' Target Market and Value Creation

The global crypto asset custody market is estimated at around US$ 2.0 billion in 2024 and is projected to reach US$ 2.5 billion by 2030, growing at an annual rate of 4% (Research and Markets, 2025). This growth reflects increasing institutional adoption of digital assets and the need for safe and compliant storage solutions. Fireblocks positions itself at the centre of this market by supporting institutions seeking to transition into digital finance without developing complex blockchain systems internally.

Fireblocks' Main Advantages and Competitive Strategy

Core Advantages

Fireblocks' competitive advantage comes from its highly secure technology, large network of institutional users, and strict focus on regulation. Its multi-party computation (MPC) technology protects digital assets by splitting each security key into several parts, so there is never one single point that can be hacked or stolen (Fireblocks, 2024). This is a key differentiator from traditional multi-signature systems, which are more vulnerable to breaches (CCN, 2024). As a result, financial institutions such as banks, asset managers, and exchanges can confidently manage, store, and transfer digital assets at scale.

The company's growing institutional network generates powerful network effects that strengthen customer retention and create barriers to entry (Yahoo Finance, 2024). Every new client connected to the Fireblocks platform adds value for others by expanding the pool of trusted transaction partners. Additionally, Fireblocks' broad service offering, such as custody, wallet management, tokenization, and stablecoin payment infrastructure, enables institutions to integrate digital asset operations through a single platform (Fireblocks, 2024). Its embedded compliance tools, such as AML screening and Travel Rule support, further enhance its attractiveness to regulated entities (Cointelegraph, 2023). Together, these strengths establish Fireblocks as a secure, scalable, and institution-grade digital asset platform.

Competitive Dynamics: Incumbents and New Entrants

In the digital asset custody and infrastructure market, Fireblocks stands out by combining strong technology with a connected network of partners. Compared with traditional financial institutions, it is faster to adapt and has deeper experience working with digital assets and blockchain systems, areas where traditional organisations struggle. Traditional banks often struggle to adopt blockchain infrastructure; therefore, rely on Fireblocks to access digital asset capabilities rapidly through white-labeled integrations. For instance, partnerships with BNY Mellon and ANZ prove how Fireblocks serves as an enabler rather than a disruptor of incumbent financial models (Cointelegraph, 2023).

Compared to other crypto competitors, such as BitGo, Anchorage, and Copper, Fireblocks differentiates itself through MPC-based security, global reach, and developer-friendly APIs (Fireblocks, 2024). BitGo relies on multi-signature wallets, which Fireblocks has publicly identified as less resilient against advanced cyberattacks (CCN, 2024). Anchorage, although a regulated U.S. company, has a narrower market focus on North America, while Fireblocks' infrastructure serves clients across Europe, North America, and the Asia-Pacific region (Yahoo Finance, 2024).

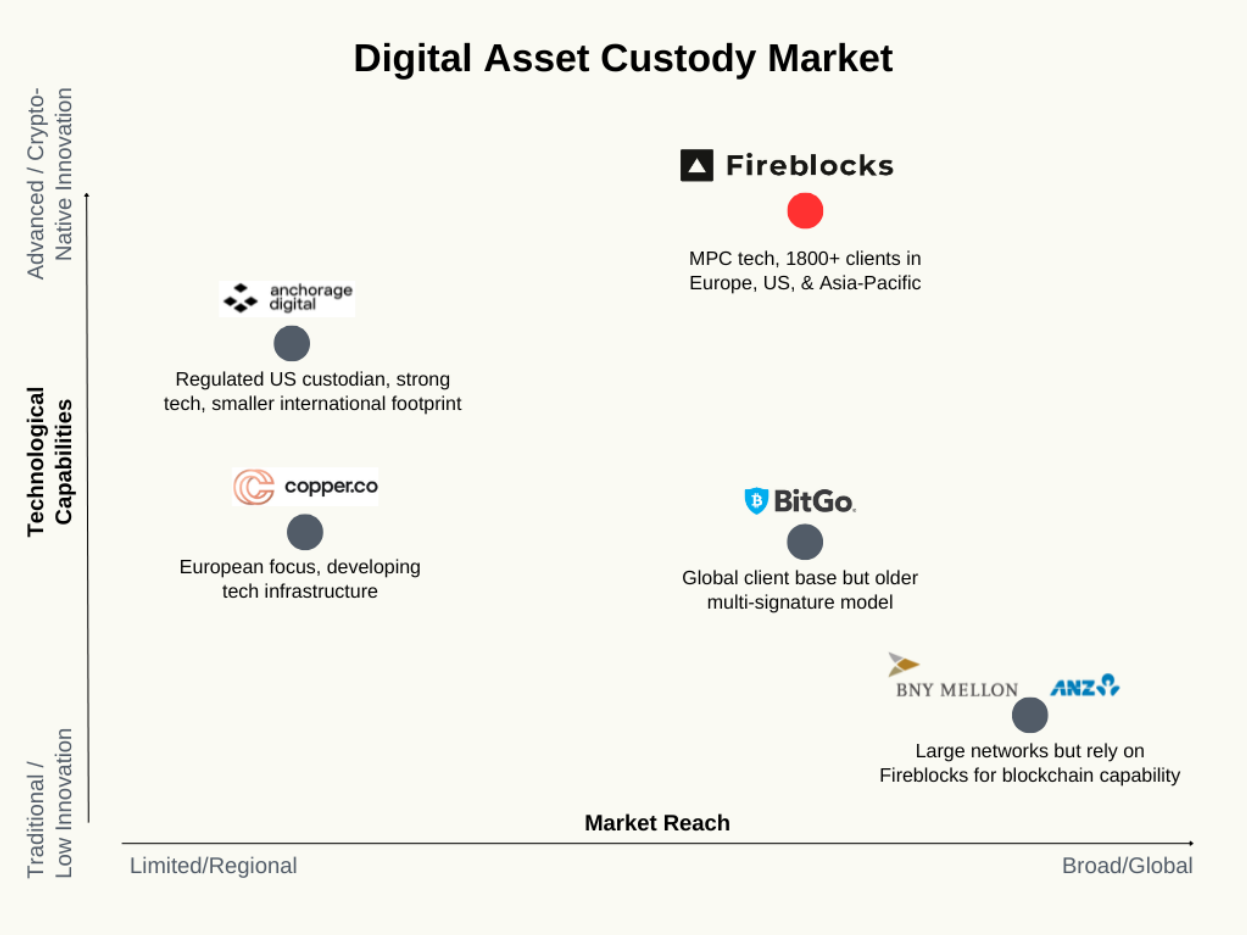


Figure 4: Fireblocks' Position in the Digital Asset Custody Market

Fireblocks' highly secure offerings and compliance orientation form significant barriers for new entrants. Replicating its scale, customer trust, and regulatory credibility requires substantial investment and time. Furthermore, Fireblocks leverages a cooperative competition ("co-opetition") strategy, partnering with incumbents rather than directly displacing them (Brandenburger & Nalebuff, 1996). This approach allows it to expand market presence while maintaining its identity as a fintech innovator. Although rising regulatory scrutiny and fast-moving innovation pose risks, Fireblocks' strong institutional partnerships and technological lead provide a durable competitive position within the digital asset economy.

Regulatory Environment

Overview

Fireblocks builds the safety rails for institutions that hold or move digital assets. It is not an exchange or broker, so the licenses belong to its clients (banks, brokers, exchanges, and e-money firms). Fireblocks provides auditable, security-certified controls that licensed firms use to meet regulatory standards (Fireblocks, n.d.-a). It follows a compliance-first approach, holding ISO 27001/27017/27018, SOC 1/2 Type II, and CCSS certifications. It has also been independently audited to CCSS-QSP Level 3 for key generation and wallet management (Fireblocks, 2024a). These controls align with AML/CTF expectations for virtual-asset providers, including licensing, KYC, transaction monitoring, suspicious reporting, and FATF Travel Rule requirements for sender and receiver data (Schwarz et al., 2021a, 2021b; Choo, 2014).

Global Regulatory Frameworks

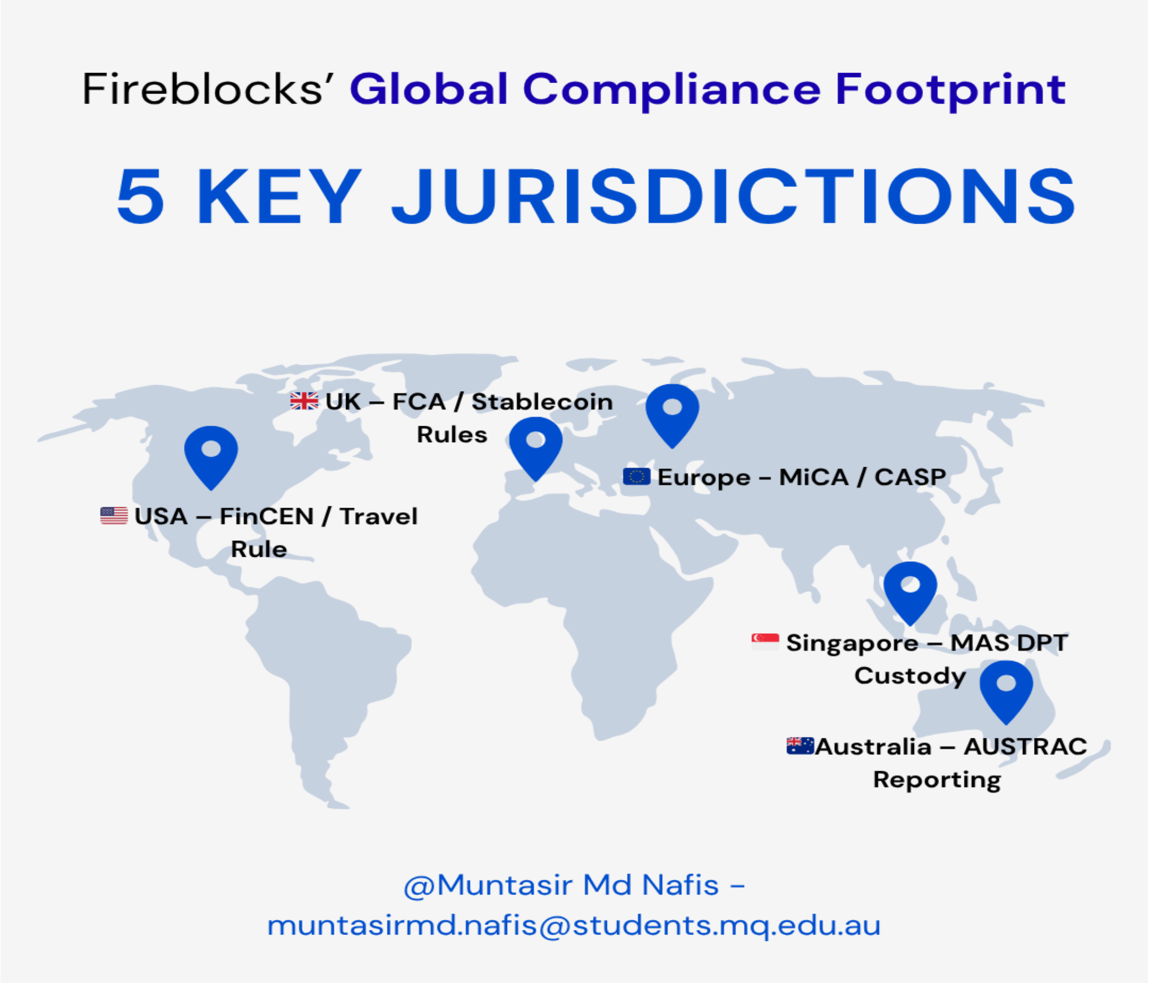

Fireblocks' Global Compliance Footprint
5 KEY JURISDICTIONS
UK – FCA / Stablecoin Rules
Europe – MiCA / CASP
USA – FinCEN / Travel Rule
Singapore – MAS DPT Custody
Australia – AUSTRAC Reporting
@Muntasir Md Nafis – muntasirmd.nafis@students.mq.edu.au

Figure 5: Global Compliance Footprint

Region	Regulator / Framework	Key Requirements	Fireblocks' Alignment
European Union	ESMA – Markets in Crypto-Assets (MiCA)	CASPs must safeguard assets, ensure governance, and comply with reporting obligations.	Provides custody technology and audit trails for authorised CASP clients (ESMA, 2025).

United Kingdom	FCA – Stablecoin Custody (CP25/14) & Regulatory Sandbox	Authorization and custody rules for stablecoins; supervised pilot testing.	Enables firms like Revolut to test Fireblocks-based systems in FCA's sandbox (FCA, 2025a; FCA, n.d.-a).
Singapore	MAS – Payment Services Act (2024)	DPT custody, cross-border transfer regulation, segregation of client assets, AML/CTF compliance.	Fireblocks supports segregation, AML/CTF checks, and secure transfers (MAS, 2024).
United States	FinCEN – CVC Guidance (2019)	MSB registration, BSA/AML program, KYC, and Travel Rule compliance.	Integrates RegTech tools to meet these requirements (FinCEN, 2019).
Australia	AUSTRAC – AML/CTF Act	Maintain AML/CTF program, KYC, file TTR/IFTI/SMR reports, and retain records.	Uses policy controls and logs to support compliance evidence (AUSTRAC, n.d.-a–f).

Table 2: Global Regulatory Frameworks and Fireblocks' Compliance Alignment

At a glance:

- EU & UK - Fireblocks supports licensed institutions (CASP, FCA).
- Singapore - Enables regulated custody and AML segregation.
- U.S.A - Aligns with FinCEN MSB and Travel Rule obligations.
- Australia - Policy controls and audit logs support AUSTRAC reporting.

RegTech Integration

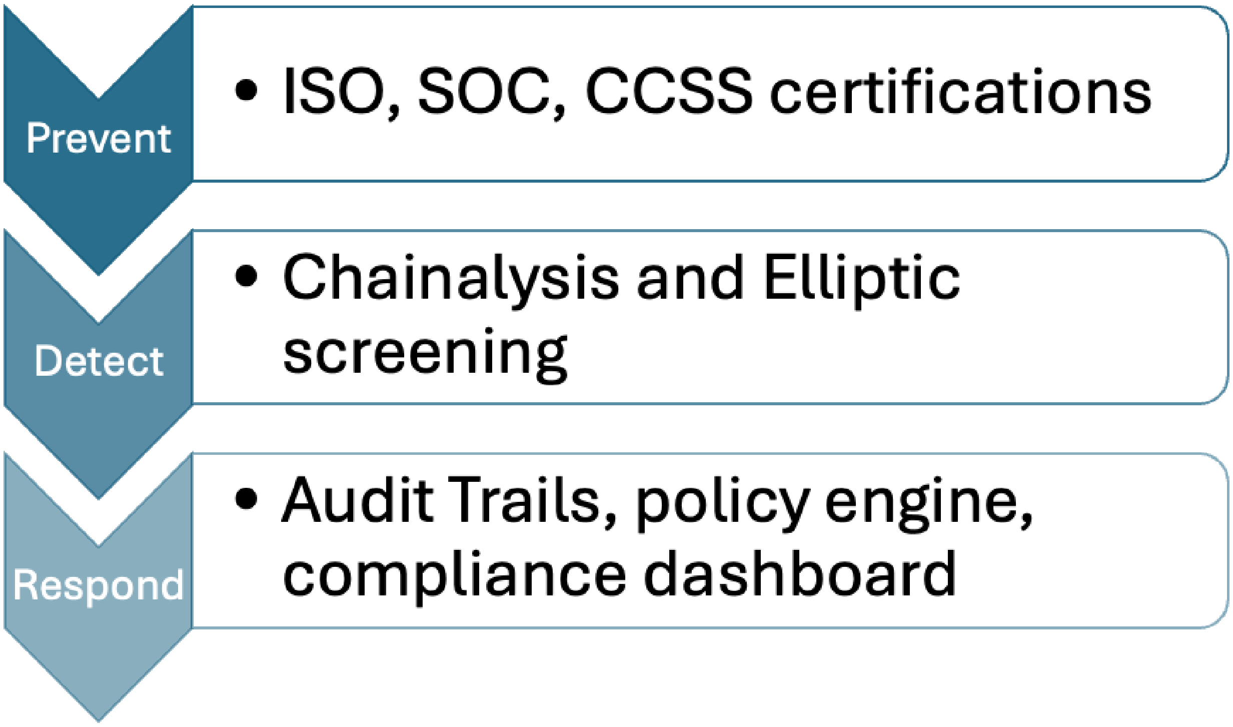

Prevent
• ISO, SOC, CCSS certifications
Detect
• Chainalysis and Elliptic screening
Respond
• Audit Trails, policy engine, compliance dashboard

Figure 6: RegTech control map

Fireblocks integrates Chainalysis and Elliptic for AML/KYT screening and risky-wallet checks, and Notabene for Travel Rule data exchange, all managed in a compliance dashboard with policy-based approvals (Fireblocks, n.d.-b; Fireblocks, 2020; Fireblocks, 2023). BNY Mellon uses Fireblocks to meet bank-grade security (BNY Mellon, 2023), and Revolut leverages it for FCA-supervised operations (Fireblocks, 2021a; Fireblocks, n.d.-c). Regulation protects users but can slow launches; Fireblocks reduces friction by embedding these rules into every transaction, supporting global compliance and operational trust (Schwarz et al., 2021a, 2021b; Anzola & dos Santos, 2022; Kaal & Howe, 2023).

Key Business Risks & Responses

Overview

Fireblocks faces multiple business risks across operational, regulatory, market, and third-party domains. Each is addressed through strong technical controls, compliance integration, and partnerships with regulated institutions, aligning with the RegTech risk mitigation framework of prevention, detection, and resilience.

Risk Matrix

Likelihood → / Impact ↓	Low Impact	High Impact
High Likelihood	Regulatory Risk – evolving global crypto frameworks (EU MiCA, MAS PSA, FinCEN CVC, AUSTRAC).	Operational Risk – potential cybersecurity breach or key compromise.
Low Likelihood	Market Risk – crypto-asset volatility and fee cycles.	Third-Party Risk – dependence on audited cloud and partner systems.

Table 3: Risk Matrix

Detailed Risk Analysis

- **Operational risk:** Cybersecurity breaches or system compromise could disrupt client operations or cause asset loss. To mitigate this, Fireblocks employs a secure multi-party computation (MPC) architecture, along with policy-based approvals and audit logging. The company maintains ISO 27001/27017/27018 and SOC 1/2 Type II certifications and has achieved CCSS-QSP Level 3, confirming independent verification of wallet generation, key storage, and transaction workflows (Fireblocks, 2024a). These layered controls reduce the risk of unauthorized access or data compromise (Fireblocks, n.d.-a).

- **Regulatory risk:** The crypto landscape is evolving, with varying frameworks such as the EU's MiCA**,** MAS's Payment Services Act**,** FinCEN's CVC guidance**,** and AUSTRAC's AML/CTF requirements**.** Fireblocks mitigates this by embedding compliance tools such as Chainalysis**,** Elliptic, and Notabene that automate AML, KYT, and Travel Rule monitoring (Fireblocks, n.d.-b; Fireblocks, 2020; Fireblocks, 2023). Partnerships with BNY Mellon and Revolut, both regulated financial institutions, further demonstrate alignment with strict supervisory standards (BNY Mellon, 2023; Fireblocks, 2021a).
- **Market risk:** Volatility in digital-asset markets can impact transaction volumes and client demand. Fireblocks minimizes exposure by focusing on B2B infrastructure**,** not speculative trading, and serving a diversified global client base including banks, exchanges, and fintech firms ensuring steady revenue through technology provision rather than market speculation (Fireblocks, n.d.-a; Fireblocks, n.d.-d).
- **Third-party risk:** Dependence on external cloud providers and partners introduces operational vulnerabilities. Fireblocks addresses this through independent audits**,** penetration testing, and redundant systems verified under SOC 2 and ISO frameworks. Institutional trust from clients such as BNY Mellon and Amber Group illustrates strong supplier-risk management and resilience (Fireblocks, n.d.-a; BNY Mellon, 2023).

Collectively, Fireblocks' embedded compliance, external audits, and institutional partnerships demonstrate a proactive RegTech approach keeping residual risk moderate yet well-controlled within global regulatory standards.

Conclusion

Fireblocks is a remarkable investment opportunity in the quickly growing industry for digital asset infrastructure. It was founded by cybersecurity specialists and uses a unique multi-party computation (MPC) and confidential computing architecture to provide enterprise-grade security and regulatory compliance. Such solutions remove the single points of failure and build unmatched institutional trust. With more than 2,000 customers worldwide, from top banks to fintech businesses, Fireblocks has become a necessary infrastructure to securely transfer digital assets worldwide. Its compliance with worldwide regulatory frameworks such as AUSTRAC, MAS, FCA, and MiCA only goes further to build investor confidence and vouches for the scalability of Fireblocks safely across borders. Although competition and regulations remain essential risks, the culture of compliance, innovation, and market momentum established for Fireblocks provides potent antidotes.

In summary, investing in Fireblocks offers investors strategic exposure to one of the most secure and scalable infrastructures in the financial technology sector. Its leadership in technology, an expanding institutional network, and resilience across market cycles make Fireblocks a valuable and future-ready investment for those seeking long-term growth and stability in digital finance.

References

Amazon Web Services. (2023). *Build secure multi-party computation (MPC) wallets using AWS Nitro Enclaves*. https://aws.amazon.com/blogs/web3/build-secure-multi-party-computation-mpc-wallets-using-aws-nitro-enclaves/

Anzola, A., & dos Santos, M. O. T. (2022). The regulation of money laundering and corporate criminal responsibility in Spain: Compliance as a key for virtual asset service providers. *Revista Brasileira de Direito Processual Penal,* *8*(3), 1335–1370.https://doi.org/10.22197/rbdpp.v8i3.730

AUSTRAC. (n.d.-a). *Digital currency (cryptocurrency).* https://www.austrac.gov.au/business/your-industry/digital-currency-cryptocurrency

AUSTRAC. (n.d.-b). *AML/CTF programs.* https://www.austrac.gov.au/business/core-guidance/amlctf-programs

AUSTRAC. (n.d.-c). *Customer identification and verification.* https://www.austrac.gov.au/business/core-guidance/customer-identification-and-verification

AUSTRAC. (n.d.-d). *Reporting.* https://www.austrac.gov.au/business/core-guidance/reporting

AUSTRAC. (n.d.-e). *Record-keeping.* https://www.austrac.gov.au/business/core-guidance/record-keeping

AUSTRAC. (n.d.-f). *Preventing financial crime using a risk-based approach.* https://www.austrac.gov.au/business/core-guidance/preventing-financial-crime-using-risk-based-approach

BNY Mellon. (2023). *BNY Mellon launches new digital asset custody platform.* https://www.bny.com/corporate/global/en/about-us/newsroom/press-release/bny-mellon-launches-new-digital-asset-custody-platform-130305.html

Brandenburger, A. M., & Nalebuff, B. J. (1996). *Co-opetition.* Crown Business.

CCN. (2024). *Fireblocks vs BitGo: Security architecture comparison*. Retrieved from https://www.ccn.com/education/crypto/fireblocks-payment-network-xrp-vs-swift

Choo, K.-K. R. (2014). Designated non-financial businesses and professionals: A review and analysis of recent financial action task force on money laundering mutual evaluation reports. *Security Journal, 27*(1), 1–26. https://doi.org/10.1057/sj.2012.9

Cointelegraph. (2023). *Fireblocks launches institutional custody partnerships*. Retrieved from https://cointelegraph.com/news/fireblocks-galaxy-bakkt-institutional-crypto-custody

Economic Times. (2025, October 15). Bitcoin and Ethereum drop below key support levels; crypto market cap slips under $3.8 trillion. https://m.economictimes.com/markets/cryptocurrency/bitcoin-and-ethereum-drop-below-key-support-levels-crypto-market-cap-slips-under-3-8-trillion/articleshow/124620785.cms?

European Securities and Markets Authority. (2025). *Supervisory briefing on authorisation of CASPs (ESMA75-453128700-1263).* https://www.esma.europa.eu/sites/default/files/2025-01/ESMA75-453128700-1263_Supervisory_Briefing_on_Authorisation_of_CASPs.pdf

Evans, D. (2025, February 15). Are cross border crypto payments the future of international transfers? *Fireblocks Blog*. Retrieved from https://www.fireblocks.com/blog/are-cross-border-payments-ripe-for-disruption/

Erinle, Y., Feng, Y., Xu, J., Vadgama, N., & Tasca, P. (2025). Shared-Custodial Wallet for Multi-Party Crypto-Asset Management. *Future Internet*, *17*(1), Article 7. https://doi.org/10.3390/fi17010007

Financial Conduct Authority. (2025a). *CP25/14: Stablecoin issuance and cryptoasset custody.* https://www.fca.org.uk/publications/consultation-papers/cp25-14-stablecoin-issuance-cryptoasset-custody

Financial Conduct Authority. (n.d.-a). *Regulatory sandbox.* https://www.fca.org.uk/firms/innovation/regulatory-sandbox

Financial Crimes Enforcement Network. (2019). *Application of FinCEN's regulations to certain business models involving convertible virtual currencies.* https://www.fincen.gov/system/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf

Fireblocks. (2020). *Introducing automated AML & KYT screening with Chainalysis / How to build a secure and compliant cryptocurrency business.* https://www.fireblocks.com/blog/fireblocks-chainalysis-how-to-build-a-secure-and-compliant-cryptocurrency-business/

Fireblocks. (2021a). *Announcing Revolut—our 100th customer.* https://www.fireblocks.com/blog/announcing-revolut-our-100th-customer/

Fireblocks. (2023). *Introducing Fireblocks Compliance Solutions Suite + Notabene Travel Rule integration.* https://www.fireblocks.com/blog/introducing-fireblocks-compliance-solutions-suite-notabene-travel-rule-integration/

Fireblocks. (2024). *Fireblocks DeFi suite: Institutional digital asset security*. https://www.fireblocks.com/blog/fireblocks-defi-suite-institutional-digital-asset-security-2024/

Fireblocks. (2024). *Technology overview and MPC security architecture*. Retrieved from https://www.fireblocks.com

Fireblocks. (2024a). *Fireblocks achieves first ever CCSS-QSP Level 3 certification.* https://www.fireblocks.com/blog/fireblocks-achieves-first-ever-ccss-qsp-level-3-certification/

Fireblocks. (2025). *Understanding Hong Kong's virtual asset trading platform licensing: A strategic overview.* https://www.fireblocks.com/blog/hong-kong-virtual-asset-trading-platform-licensing-strategic-overview/

Fireblocks. (2025a). *About Fireblocks.* Retrieved from https://www.fireblocks.com/about/ Fireblocks. (2025b). *Leading digital asset infrastructure.* Retrieved from https://www.fireblocks.com/

Fireblocks. (2025c). *Secure multi-party computation framework.* Retrieved from https://www.fireblocks.com/secure-multi-party-computation-framework/

Fireblocks. (n.d.-a). *Fireblocks.* https://www.fireblocks.com/

Fireblocks. (n.d.-b). *Compliance integrations (Chainalysis, Elliptic, Notabene).* https://www.fireblocks.com/platforms/compliance/

Fireblocks. (n.d.-c). *Revolut (customer page).* https://www.fireblocks.com/customers/revolut/

Fireblocks. (n.d.-d). *Amber Group and Fireblocks extend partnership for crypto asset security.* https://www.fireblocks.com/press/amber-group-and-fireblocks-extend-partnership-for-crypto-asset-security/

Forbes. (2022, January 27). Crypto custodian Fireblocks raises $550 million at $8 billion valuation. Retrieved from https://www.forbes.com/sites/ninabambysheva/2022/01/27/crypto-custodian-fireblocks-raises-550-million-at-8-billion-valuation/

Kaal, W. A., & Howe, H. A. (2023). Custody of digital assets. *Jurimetrics, 63*(2), 169–195.

Kroweski, J. (2023, July 15). *Integrating Fireblocks security into Injective* [Infographic]. Medium. https://medium.com/@kroweski/integrating-fireblocks-security-into-injective-e17dd327e51d

Marciano, I. (2025, May 21). *Introducing MPC-cmp: Pushing MPC wallet signing speeds 8x*. Fireblocks. https://www.fireblocks.com/blog/pushing-mpc-wallet-signing-speeds-8x-with-mpc-cmp-9/

Microsoft. (2024). *Fireblocks partners with Azure Confidential Computing for institutional digital asset security*. https://www.microsoft.com/en/customers/story/1668023878965255083-fireblocks-partner-professional-services-azure-confidential-computing-infra

Monetary Authority of Singapore. (2024). *MAS expands scope of regulated payment services.* https://www.mas.gov.sg/news/media-releases/2024/mas-expands-scope-of-regulated-payment-services

Report: Fireblocks Business Breakdown & Founding Story | Contrary Research. (2018). Contrary.com. https://research.contrary.com/company/fireblocks

Research and Markets. (2025, June 27). Crypto Asset Management Market Trends and Investment Opportunities 2025-2030 - Growth in DeFi and Tokenization Drives Demand for Crypto Asset Management Tools in Decentralized Markets. Yahoo Finance. https://uk.finance.yahoo.com/news/crypto-asset-management-market-trends-080400840.html

Lim, H. J., Lee, S., Kim, M., & Lee, W. (2025). Comparative Analysis of Security Features and Risks in Digital Asset Wallets. Electronics (Basel), 14(12), Article 2436. https://doi.org/10.3390/electronics14122436

Schwarz, N., Chen, K., Fernando, F., Jackson, G., Kao, K., Markevych, M., & Poh, K. (2021a). Virtual assets and anti-money laundering and combating the financing of terrorism (1): Some legal and practical considerations. International Monetary Fund.

Schwarz, N., Chen, K., Fernando, F., Jackson, G., Kao, K., Markevych, M., & Poh, K. (2021b). Virtual assets and anti-money laundering and combating the financing of terrorism (2): Effective AML/CTF regulatory and supervisory framework—Some legal and practical considerations. International Monetary Fund.

Yahoo Finance. (2024). *Fireblocks expansion and institutional adoption*. Retrieved from https://finance.yahoo.com/news/fireblocks-expands-institutional-digital-asset-offering

Zhong, H., Sang, Y., Zhang, Y., & Xi, Z. (2020). Secure multi-party computation on blockchain: An overview. In H. Shen & Y. Sang (Eds.), *Parallel architectures, algorithms and programming* (pp. 452–460). Springer. https://doi.org/10.1007/978-981-15-2767-8_40